AF
ZW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application No.: 09/930,384
Filed: August 15, 2001
Inventor(s):
King et al.

Title: PORTABLE NETWORK ENCRYPTION KEYS

Examiner: Khoshnoodi, Nadia
Group/Art Unit: 2137
Atty. Dkt. No: 5681-04200

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents, Alexandria, VA 22313-1450, on the date indicated below.

B. Noël Kivlin

Signature — December 18, 2006 — Date

AMENDED APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir/Madam:

Further to the Notice of Appeal filed July 10, 2006 and in response to the Notification of Non-Compliant Appeal Brief of November 17, 2006, Appellants present this Amended Appeal Brief. Appellants respectfully request that this appeal be considered by the Board of Patent Appeals and Interferences.

I. REAL PARTY IN INTEREST

As evidenced by the assignment recorded at Reel/Frame 012533/0594, the subject application is owned by Sun Microsystems, Inc., a corporation organized and existing under and by virtue of the laws of the State of Delaware, and now having its principal place of business at 4150 Network Circle, Santa Clara, CA 95054.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to Appellants, Appellants' legal representatives, or assignee which will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1 – 25 and 27 – 36 are pending. Claim 26 has been canceled. Claims 1 – 25 and 27 – 36 are rejected, and the rejection of these claims is being appealed. A copy of claims 1 – 25 and 27 – 36 is included in the Claims Appendix attached hereto.

IV. STATUS OF AMENDMENTS

Amendments to claims 21 – 25, 27, and 28, having been submitted subsequent to the final rejection in an Amendment dated June 12, 2006, have been entered. No other amendments to the claims have been submitted subsequent to the final rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a portable storage device (see, e.g., FIGs. 4 and 17, reference numeral 54; page 12, line 28 – page 13, line 16) containing network identification information (see, e.g., page 10, lines 12 – 29) for a processing unit (see, e.g., FIG. 3, reference numerals 22 and 22'; page 10, line 5 – page 11, line 26). The processing unit is connectable to a data communications network (see, e.g., FIG. 1, reference numerals 2 and 3; page 9, lines 3 – 22). The processing unit includes a device reader (see, e.g., FIG. 4, reference numeral 40; page 12, lines 4 – 26) configured to read the portable storage device. The portable storage device comprises storage (see, e.g., FIG. 4, reference numeral 58; page 12, lines 28 – 30; page 19, line 28 – page 20, line 5). The storage is configured to store a network identity (see, e.g., page 10, lines 12 – 29) for the processing unit and at least one encryption key (see, e.g., page 25, line 11 – page 26, line 10). The portable storage device also comprises an access controller (see, e.g., FIG. 4, reference numeral 59; FIG. 9, reference numeral 160; page 12, line 30 – page 13, line 2; page 19, lines 22 – 23) which is operable to control access to the storage by implementing key-key encryption (see, e.g., FIG. 9, reference numeral 160; page 19, lines 22 – 23; page 20, lines 7 – 14; page 26, line 10 – page 28, line 14).

Independent claim 13 is directed to a processing unit (see, e.g., FIG. 3, reference numerals 22 and 22'; page 10, line 5 – page 11, line 26) connectable to a data communications network (see, e.g., FIG. 1, reference numerals 2 and 3; page 9, lines 3 – 22). The processing unit comprises a device reader (see, e.g., FIG. 4, reference numeral 40; page 12, lines 4 – 26) for a portable storage device (see, e.g., FIGs. 4 and 17, reference numeral 54; page 12, line 28 – page 13, line 16). The portable storage device comprises storage (see, e.g., FIG. 4, reference numeral 58; page 12, lines 28 – 30; page 19, line 28 – page 20, line 5) and an access controller (see, e.g., FIG. 4, reference numeral 59; FIG. 9, reference numeral 160; page 12, line 30 – page 13, line 2; page 19, lines 22 – 23). The storage holds a network identity (see, e.g., page 10, lines 12 – 29) for the processing unit and at least one encryption key (see, e.g., page 25, line 11 – page 26, line 10). The access controller controls access to the storage by implementing key-key

encryption (see, e.g., FIG. 9, reference numeral 160; page 19, lines 22 – 23; page 20, lines 7 – 14; page 26, line 10 – page 28, line 14). The processing unit is operable to access a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller (see, e.g., FIG. 11, reference numeral 190; FIG. 12, reference numeral 290; page 23, lines 4 – 9; page 26, lines 16 – 21), and, in response to receipt of an access key from the access controller (see, e.g., FIG. 11, reference numeral 200; FIG. 12, reference numeral 300; page 23, lines 17 – 21; page 26, line 29 – page 27, line 3), is operable to send an encrypted command to access the content of the storage of the portable storage device (see, e.g., FIG. 11, reference numeral 202; FIG. 12, reference numeral 302; page 23, lines 23 – 26; page 27, lines 5 – 8).

Independent claim 21 is directed to a computer-readable storage medium comprising a control program (see, e.g., page 34, lines 4 – 10) for a processing unit (see, e.g., FIG. 3, reference numerals 22 and 22'; page 10, line 5 – page 11, line 26) connectable to a data communications network (see, e.g., FIG. 1, reference numerals 2 and 3; page 9, lines 3 – 22). The processing unit comprises a device reader (see, e.g., FIG. 4, reference numeral 40; page 12, lines 4 – 26) for a portable storage device (see, e.g., FIGs. 4 and 17, reference numeral 54; page 12, line 28 – page 13, line 16). The portable storage device includes storage (see, e.g., FIG. 4, reference numeral 58; page 12, lines 28 – 30; page 19, line 28 – page 20, line 5) and an access controller (see, e.g., FIG. 4, reference numeral 59; FIG. 9, reference numeral 160; page 12, line 30 – page 13, line 2; page 19, lines 22 – 23). The storage holds a network identity (see, e.g., page 10, lines 12 – 29) for the processing unit and at least one encryption key (see, e.g., page 25, line 11 – page 26, line 10). The access controller controls access to the storage by implementing key-key encryption (see, e.g., FIG. 9, reference numeral 160; page 19, lines 22 – 23; page 20, lines 7 – 14; page 26, line 10 – page 28, line 14). The control program is executable to implement: accessing a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller (see, e.g., FIG. 11, reference numeral 190; FIG. 12, reference numeral 290; page 23, lines 4 – 9; page 26, lines 16 – 21); and in response to receipt of an access key from the access controller (see, e.g., FIG. 11, reference numeral 200; FIG. 12, reference numeral 300; page 23, lines 17 – 21; page

26, line 29 – page 27, line 3), sending an encrypted command to access the content of the storage of the portable storage device (see, e.g., FIG. 11, reference numeral 202; FIG. 12, reference numeral 302; page 23, lines 23 – 26; page 27, lines 5 – 8).

Independent claim 29 is directed to a microcontroller (see, e.g., FIG. 3, reference numerals 22 and 22'; page 5, lines 25 – 29; page 10, line 5 – page 11, line 26) connectable to a data communications network (see, e.g., FIG. 1, reference numerals 2 and 3; page 9, lines 3 – 22). The microcontroller comprises a device reader (see, e.g., FIG. 4, reference numeral 40; page 12, lines 4 – 26) for a portable storage device (see, e.g., FIGs. 4 and 17, reference numeral 54; page 12, line 28 – page 13, line 16). The portable storage device includes storage (see, e.g., FIG. 4, reference numeral 58; page 12, lines 28 – 30; page 19, line 28 – page 20, line 5) and an access controller (see, e.g., FIG. 4, reference numeral 59; FIG. 9, reference numeral 160; page 12, line 30 – page 13, line 2; page 19, lines 22 – 23). The storage holds a network identity (see, e.g., page 10, lines 12 – 29) for the microcontroller and at least one encryption key (see, e.g., page 25, line 11 – page 26, line 10). The access controller controls access to the storage by implementing key-key encryption (see, e.g., FIG. 9, reference numeral 160; page 19, lines 22 – 23; page 20, lines 7 – 14; page 26, line 10 – page 28, line 14). The microcontroller also comprises a control program (see, e.g., page 34, lines 4 – 10) which is operable to access a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller (see, e.g., FIG. 11, reference numeral 190; FIG. 12, reference numeral 290; page 23, lines 4 – 9; page 26, lines 16 – 21), and, in response to receipt of an access key from the access controller (see, e.g., FIG. 11, reference numeral 200; FIG. 12, reference numeral 300; page 23, lines 17 – 21; page 26, line 29 – page 27, line 3), is operable to send an encrypted command to access the content of the storage of the portable storage device (see, e.g., FIG. 11, reference numeral 202; FIG. 12, reference numeral 302; page 23, lines 23 – 26; page 27, lines 5 – 8).

Independent claim 30 is directed to a server computer (see, e.g., FIG. 3, reference numerals 22 and 22'; page 5, lines 25 – 29; page 10, line 5 – page 11, line 26) which comprises a device reader (see, e.g., FIG. 4, reference numeral 40; page 12, lines 4 – 26)

configured to read a portable storage device (see, e.g., FIGs. 4 and 17, reference numeral 54; page 12, line 28 – page 13, line 16). The server computer also comprises a microcontroller which is operable as a service processor (see, e.g., FIG. 3, reference numerals 22 and 22'; page 5, lines 25 – 29; page 10, line 5 – page 11, line 26). The microcontroller is connected to read the content of storage (see, e.g., FIG. 4, reference numeral 58; page 12, lines 28 – 30; page 19, line 28 – page 20, line 5) mounted in the portable storage device. The microcontroller comprises a control program (see, e.g., page 34, lines 4 – 10) for a processing unit (see, e.g., FIG. 3, reference numerals 22 and 22'; page 10, line 5 – page 11, line 26) connectable to a data communications network (see, e.g., FIG. 1, reference numerals 2 and 3; page 9, lines 3 – 22). The processing unit has a device reader (see, e.g., FIG. 4, reference numeral 40; page 12, lines 4 – 26) for the portable storage device. The portable storage device includes storage (see, e.g., FIG. 4, reference numeral 58; page 12, lines 28 – 30; page 19, line 28 – page 20, line 5) and an access controller (see, e.g., FIG. 4, reference numeral 59; FIG. 9, reference numeral 160; page 12, line 30 – page 13, line 2; page 19, lines 22 – 23). The storage holds a network identity (see, e.g., page 10, lines 12 – 29) for the processing unit and at least one encryption key (see, e.g., page 25, line 11 – page 26, line 10). The access controller controls access to the storage by implementing key-key encryption (see, e.g., FIG. 9, reference numeral 160; page 19, lines 22 – 23; page 20, lines 7 – 14; page 26, line 10 – page 28, line 14). The control program is operable to access a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller (see, e.g., FIG. 11, reference numeral 190; FIG. 12, reference numeral 290; page 23, lines 4 – 9; page 26, lines 16 – 21), and, in response to receipt of an access key from the access controller (see, e.g., FIG. 11, reference numeral 200; FIG. 12, reference numeral 300; page 23, lines 17 – 21; page 26, line 29 – page 27, line 3), is operable to send an encrypted command to access the content of the storage of the portable storage device (see, e.g., FIG. 11, reference numeral 202; FIG. 12, reference numeral 302; page 23, lines 23 – 26; page 27, lines 5 – 8).

Independent claim 31 is directed to a method for securing encryption keys for use in a processing unit (see, e.g., FIG. 3, reference numerals 22 and 22'; page 10, line 5 –

page 11, line 26) connectable to a data communications network (see, e.g., FIG. 1, reference numerals 2 and 3; page 9, lines 3 – 22). The method comprises providing a portable storage device (see, e.g., FIGs. 4 and 17, reference numeral 54; page 12, line 28 – page 13, line 16) for a processing unit (see, e.g., FIG. 3, reference numerals 22 and 22'; page 10, line 5 – page 11, line 26), wherein the processing unit is connectable to the data communications network, wherein the processing unit comprises a device reader (see, e.g., FIG. 4, reference numeral 40; page 12, lines 4 – 26) configured to read the portable storage device, and wherein the portable storage device comprises storage (see, e.g., FIG. 4, reference numeral 58; page 12, lines 28 – 30; page 19, line 28 – page 20, line 5) and an access controller (see, e.g., FIG. 4, reference numeral 59; FIG. 9, reference numeral 160; page 12, line 30 – page 13, line 2; page 19, lines 22 – 23). The method also comprises providing in the storage a network identity (see, e.g., page 10, lines 12 – 29) for the processing unit and at least one encryption key (see, e.g., page 25, line 11 – page 26, line 10). The method further comprises implementing key-key encryption in the access controller for controlling access to the storage (see, e.g., FIG. 9, reference numeral 160; page 19, lines 22 – 23; page 20, lines 7 – 14; page 26, line 10 – page 28, line 14).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1 – 25 and 27 – 36 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Sehr (U.S. Patent No. 6,085,976) and further in view of Houvener et al. (U.S. Pub. No. 2002/0138351, hereinafter "Houvener").

VII. ARGUMENT

First Ground of Rejection:

Claims 1 – 25 and 27 – 36 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Sehr (U.S. Patent No. 6,085,976) and further in view of Houvener et al.

(U.S. Pub. No. 2002/0138351, hereinafter "Houvener"). Appellants traverse this rejection for the following reasons.

Claims 1 – 12 and 31 – 36:

To establish a *prima facie* obviousness of a claimed invention, all claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 U.S.P.Q. 580 (C.C.P.A. 1974), MPEP 2143.03. Appellants respectfully submit that the cited references, taken individually or in combination, do not teach or suggest all the limitations recited in the claims.

In particular, Appellants respectfully submit that the cited references, taken individually or in combination, do not teach or suggest a "portable storage device comprising: storage, the storage configured to store a network identity for the processing unit" as recited in claim 1. Sehr teaches a portable card which stores various kinds of user-specific information but not a network identity for a processing unit. For example, at column 6, lines 26 – 31, Sehr states:

> The data stored in the card includes the equivalent of an electronic ticket for a particular itinerary, use rights for a specific transportation carrier, considerations for travel-related services, electronic money for payment, or security information for protecting the card content and identifying the rightful card holder.

Therefore, while the contents of Sehr's card may be usable to identify a person in possession of the card, there is no teaching or suggestion in Sehr that the card may store any information usable as a network identity for a processing unit.

Likewise, Houvener also fails to teach or suggest a portable storage device comprising storage which is configured to store a network identity for a processing unit. In paragraphs [0027] – [0033], Houvener discloses an identification terminal which is configured to read and verify various forms of user identification from external sources such as credit cards, ID cards, check routing numbers, etc. Once the user identification from the

external source has been entered into the terminal, the terminal may use a computer network to contact a remote database for verification of the user identification. In accessing the network, the terminal may identify itself by supplying a MAC address or other unique identifier "derived from local hardware." It is this pre-existing identifier stored in local hardware, not the user identification information provided by an external source, that is used to access the network in Houvener. Therefore, the user identification information stored on a card does not comprise a network identity. Any network identification information or network identity in Houvener (e.g., a MAC address) is stored in the terminal itself prior to the reading of any card, and therefore the network identification information or network identity is not stored in any card or other portable element supplied by a user of Houvener's terminal. Accordingly, neither Sehr nor Houvener teaches or suggests a portable storage device comprising storage, where the storage is configured to store a network identity.

Even assuming, *arguendo*, that all the claim limitations are taught or suggested by the individual references, Appellants respectfully submit that there is no evidence of a suggestion or motivation for one of skill in the art to combine Sehr and Houvener to produce the claimed invention. As held by the U.S. Court of Appeals for the Federal Circuit in *Ecolochem Inc. v. Southern California Edison Co.*, an obviousness claim that lacks evidence of a suggestion or motivation for one of skill in the art to combine prior art references to produce the claimed invention is defective as hindsight analysis. In addition, the showing of a suggestion, teaching, or motivation to combine prior teachings "must be clear and particular .... Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence'." *In re Dembiczak*, 175 F.3d 994, 50 USPQ2d 1614 (Fed. Cir. 1999). As the Advisory Action argues:

> Houvener et al. suggest that it is beneficial for a device to contain a network id in order to determine whether or not a specific device should be granted access to various system services.... Therefore, Sehr et al. teach the portable storage with various fields for facilitating access control and secure communications and Houvener et al. suggest why one would be motivated to incorporate a network id field as one of the components of the portable storage device.

Appellants respectfully disagree. Houvener discloses a terminal which internally stores a network identification for a processing unit. Sehr discloses a portable card which stores various types of user-centric information but not a network identification for a processing unit. Appellants can find no evidence of a suggestion or motivation in the cited references to move Houvener's network identification from non-portable computer hardware to Sehr's portable storage device.

Accordingly, claim 1 and its dependent claims 2 – 12 are believed to patentably distinguish over the cited references for at least the reasons given above. Claim 31 recites features similar to those of claim 1 and is therefore believed to patentably distinguish over Sehr and Houvener for at least the reasons given above. Dependent claims 32 – 36 are also believed to patentably distinguish over the cited references for similar reasons.

Claims 13 – 25 and 27 – 30:

Claim 13 is believed to patentably distinguish over Sehr and Houvener for the reasons given above. In particular, Appellants respectfully submit that the cited references, taken individually or in combination, do not teach or suggest "the portable storage device comprising storage ... the storage holding a network identity for the processing unit" as recited in claim 13. Additionally, Appellants respectfully submit that the cited references, taken individually or in combination, do not teach or suggest "the processing unit being operable to access a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller, and, in response to receipt of an access key from the access controller, being operable to send an encrypted command to access the content of the storage of the portable storage device" as recited in claim 13. In rejecting claim 13, the Final Office Action admitted that this feature is not explicitly disclosed and argued as follows:

> However, Sehr teaches that the particular card data is protected with encryption so that only the entity intended to receive the data does so. Furthermore, Sehr teaches that the key is used to encrypt a payment form that is sent to the cardholder who can only use the form by decrypting it

> with the correct key, thereby allowing access to the payment information held in the card in order to clear the payment. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Sehr for it to be operable to access a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller, and, in response to receipt of an access key from the access controller, being operable to send an encrypted command to access the content of the storage of the portable storage device. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Sehr suggests that using a key to authorize/allow access to various data results in a stronger means of authentication in col. 17, lines 50 – 67.

As held by the U.S. Court of Appeals for the Federal Circuit in *Ecolochem Inc. v. Southern California Edison Co.*, an obviousness claim that lacks evidence of a suggestion or motivation for one of skill in the art to combine prior art references to produce the claimed invention is defective as hindsight analysis. In addition, the showing of a suggestion, teaching, or motivation to combine prior teachings "must be clear and particular .... Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence'." *In re Dembiczak*, 175 F.3d 994, 50 USPQ2d 1614 (Fed. Cir. 1999). The passage from Sehr cited by the Final Office Action discloses encrypting a payment form which can be unlocked only by a user supplying a card with the proper authenticity code. There is no teaching or suggestion in Sehr for numerous limitations recited in claim 13, such as, for example, "supplying a key-encrypted request to the access controller" or the processing unit "being operable to send an encrypted command to access the content of the storage of the portable storage device." Furthermore, Appellants can find no evidence of a suggestion or motivation to modify the authenticity code of Sehr to produce the limitations recited in claim 13. Appellants submit that the alleged motivation to modify the cited passage of Sehr to produce the claimed invention is not "clear and particular" and that the rejection of claim 13 on this basis amounts to impermissible hindsight analysis.

Accordingly, claim 13 and its dependent claims 14 – 20 are believed to patentably distinguish over the cited references for at least the reasons given above. Claims 21, 29, and

30 recite features similar to those of claim 13 and is therefore believed to patentably distinguish over Sehr and Houvener for at least the reasons given above. Dependent claims 22 – 25, 27, and 28 are also believed to patentably distinguish over the cited references for similar reasons.

For the foregoing reasons, it is submitted that the Examiner's rejection of claims 1 – 25 and 27 – 36 was erroneous, and reversal of the decision is respectfully requested.

The Commissioner is authorized to charge any fees that may be due to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 50-1505/5681-04200/BNK. This Appeal Brief is submitted with a return receipt postcard.

Respectfully submitted,

B. Noël Kivlin
Reg. No. 33,929
ATTORNEY FOR APPELLANT(S)

Meyertons, Hood, Kivlin, Kowert and Goetzel, P.C.
P.O. Box 398
Austin, Texas 78767-0398
Phone: (512) 853-8800
Date: December 18, 2006

VIII. CLAIMS APPENDIX

The claims on appeal are as follows.

1. A portable storage device containing network identification information for a processing unit, the processing unit being connectable to a data communications network and including a device reader configured to read the portable storage device, the portable storage device comprising:

storage, the storage configured to store a network identity for the processing unit and at least one encryption key; and

an access controller, the access controller being operable to control access to the storage by implementing key-key encryption.

2. The portable storage device of claim 1, comprising at least one secure storage portion accessible only under the control of the access controller.

3. The portable storage device of claim 2, wherein said at least one encryption key is held in said secure storage portion.

4. The portable storage device of claim 2, wherein at least one network security encryption key is held in said secure storage portion.

5. The portable storage device of claim 2, wherein a file is configured in said secure storage portion.

6. The portable storage device of claim 2, wherein one or more files containing information are configured in respective secure storage portions.

7. The portable storage device of claim 2, wherein the access controller is operable to perform key-key verification of a request encrypted by a request key supplied from the processing unit and, in response to the request key verifying correctly, to return

to the processing unit an access key derived from said at least one encryption key to permit access to the secure storage portion.

8. The portable storage device of claim 7, wherein the access controller is subsequently operable to respond to a command from the processing unit that is encrypted using the access key to access the secure storage portion.

9. The portable storage device of claim 2, wherein the storage in the portable storage device comprises random access memory, the secure storage comprising a part of the random access memory.

10. The portable storage device of claim 1, wherein the access controller is a programmed microcontroller.

11. The portable storage device of claim 1, wherein the portable storage device is a smart card.

12. The processing unit of claim 1, wherein the network identity comprises a MAC address.

13. A processing unit connectable to a data communications network, the processing unit comprising:

a device reader for a portable storage device, the portable storage device comprising storage and an access controller, the storage holding a network identity for the processing unit and at least one encryption key, and the access controller controlling access to the storage by implementing key-key encryption, the processing unit being operable to access a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller, and, in response to receipt of an access key from the access controller, being operable to send an encrypted command to access the content of the storage of the portable storage device.

14. The processing unit of claim 13, wherein, in response to the return of an access key, the processing unit is operable to use the access key to encrypt a command for access to a secure storage in the portable storage device.

15. The processing unit of claim 13, wherein the portable storage device is a smart card, the access controller is a microcontroller and the device reader is a smart card reader.

16. The processing unit of claim 13, wherein the network identity comprises a MAC address.

17. The processing unit of claim 13, comprising a service processor, the service processor being programmed to control reading of the portable storage device.

18. The processing unit of claim 17, wherein the service processor is a microcontroller.

19. The processing unit of claim 13, wherein the processing unit is a computer server.

20. The processing unit of claim 13, wherein the processing unit is a rack mountable computer server.

21. A computer-readable storage medium comprising a control program for a processing unit connectable to a data communications network, the processing unit comprising a device reader for a portable storage device that includes storage and an access controller, the storage holding a network identity for the processing unit and at least one encryption key, and the access controller controlling access to the storage by implementing key-key encryption, the control program being executable to implement:

accessing a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller; and

in response to receipt of an access key from the access controller, sending an encrypted command to access the content of the storage of the portable storage device.

22. The computer-readable storage medium of claim 21, wherein, in response to the return of an access key, the control program is executable to implement:

using the access key to encrypt a command for access to secure storage in the portable storage device.

23. The computer-readable storage medium of claim 21, wherein the portable storage device is a smart card, wherein the access controller is a microcontroller, and wherein the device reader is a smart card reader.

24. The computer-readable storage medium of claim 21, wherein the network identity comprises a MAC address.

25. The computer-readable storage medium of claim 21, wherein a service processor is configured to control reading of the portable storage device.

27. The computer-readable storage medium of claim 21, wherein the processing unit comprises a service processor, the control program controlling operation of the service processor.

28. The computer-readable storage medium of claim 27, wherein the service processor is a microcontroller.

29. A microcontroller connectable to a data communications network, the microcontroller comprising:

a device reader for a portable storage device that includes storage and an access controller, the storage holding a network identity for the microcontroller and at least one encryption key, and the access controller controlling access to the storage by implementing key-key encryption; and

a control program being operable to access a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller, and, in response to receipt of an access key from the access controller, being operable to send an encrypted command to access the content of the storage of the portable storage device.

30. A server computer comprising:

a device reader configured to read a portable storage device; and

a microcontroller, the microcontroller being operable as a service processor and connected to read the content of storage mounted in the portable storage device, the microcontroller comprising a control program for a processing unit connectable to a data communications network, the processing unit having a device reader for the portable storage device that includes storage and an access controller, the storage holding a network identity for the processing unit and at least one encryption key, and the access controller controlling access to the storage by implementing key-key encryption, the control program being operable to access a secure portion of the storage of the portable storage device by supplying a key-encrypted request to the access controller, and, in response to receipt of an access key from the access controller, being operable to send an encrypted command to access the content of the storage of the portable storage device.

31. A method for securing encryption keys for use in a processing unit connectable to a data communications network, the method comprising:

providing a portable storage device for a processing unit, wherein the processing unit is connectable to the data communications network, wherein the processing unit comprises a device reader configured to read the portable storage device, and wherein the portable storage device comprises storage and an access controller;

providing in the storage a network identity for the processing unit and at least one encryption key; and

implementing key-key encryption in the access controller for controlling access to the storage.

32. The method of claim 31, comprising defining at least part of the storage in the portable storage device as secure storage accessible only under the control of the access controller.

33. The method of claim 32, comprising storing said at least one encryption key in said secure storage.

34. The method of claim 32, comprising storing at least one network security encryption key in said secure storage.

35. The method of claim 31, comprising: the processing unit supplying a key-encrypted request to the access controller; the access controller providing key-key verification of the request key supplied from the processing unit; and in response to the key-encrypted request verifying correctly; returning to the processing unit an access key to permit access to the secure storage; the processing unit encrypting a command using the access key to access the secure storage; and the access controller responding to the first command to access the first storage.

36. The method of claim 31, wherein the network identity comprises a MAC address.

IX. EVIDENCE APPENDIX

No evidence submitted under 37 CFR §§ 1.130, 1.131, or 1.132 or otherwise entered by the Examiner is relied upon in this appeal.

X. RELATED PROCEEDINGS APPENDIX

There are no related proceedings known to Appellants, Appellants' legal representatives, or assignee which will directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.